

19 BUNDESREPUBLIK  
DEUTSCHLAND



DEUTSCHES  
PATENTAMT

12 Offenlegungsschrift  
10 DE 44 08 035 A 1

51 Int. Cl. 8:  
H 04 L 29/02  
H 04 L 12/22  
G 06 F 12/14

21 Aktenzeichen: P 44 08 035.2  
22 Anmeldetag: 10. 3. 94  
43 Offenlegungstag: 14. 9. 95

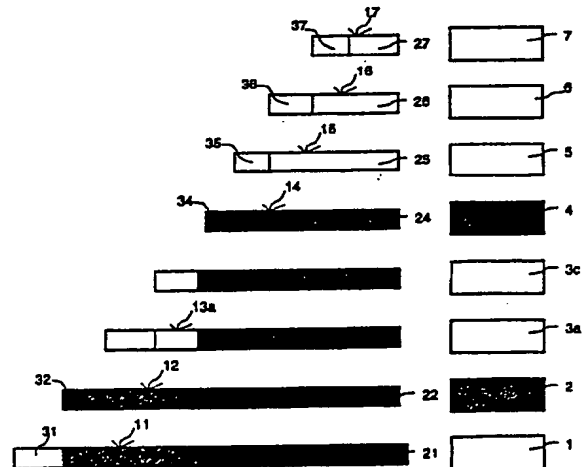
DE 44 08 035 A 1

71 Anmelder:  
Alcatel SEL Aktiengesellschaft, 70435 Stuttgart, DE  
74 Vertreter:  
Graf, G., Dipl.-Ing., Pat.-Ass., 7000 Stuttgart

72 Erfinder:  
Erbes, Norbert, Dr., 76228 Karlsruhe, DE; Doleschal,  
Bernd, Dipl.-Ing. (FH), 71665 Vaihingen, DE; Prasse,  
Christoph, Dipl.-Ing., 75428 Illingen, DE; Rother,  
Dietrich, Dr., 71732 Tamm, DE

54 Kommunikationsrechner

67 Der Kommunikationsrechner eignet sich speziell für den Betrieb in einem Rechnernetz mit einem Datenaustausch auf mehreren Schichten anhand definierter Protokolle, wie etwa dem OSI-Referenzmodell. Er enthält mehrere Prozessoren (1, 2, ..., 7), die je die Datenverarbeitung auf einer fest zugeordneten Protokollschicht übernehmen. Die zwischen dem Prozessor (2, 4) und dem Datenbus übertragenen Telegramme (12, 14) können verschlüsselt sein, ohne daß die Protokolle beeinflußt werden. Diese Maßnahme ermöglicht eine vielseitige Zugangssicherung. Die Rechner können auf beliebigen Schichten über Gateways kommunizieren, ohne rechnerintern Protokollumwandlungen vornehmen zu müssen.



DE 44 08 035 A 1

Die folgenden Angaben sind den vom Anmelder eingereichten Unterlagen entnommen

BUNDESDRUCKEREI 07. 95 508 037/319

6/30

## Beschreibung

Die Erfindung liegt auf dem Gebiet der Datenübertragung in Netzwerken und betrifft einen Kommunikationsrechner gemäß dem Oberbegriff des Patentanspruchs 1.

Datenübertragungen zwischen örtlich getrennten Datenendgeräten bedingen Vereinbarungen über die Protokolle und Telegramme, damit ein Datenaustausch in verständlicher Form stattfinden kann. In lokaler Umgebung läßt sich dies durch lokal einzuhaltende Vorschriften erreichen. Soll jedoch ein Datenaustausch zwischen Netzen mit verschiedenen Netzprotokollen stattfinden können, sind entsprechende Anpassungen der Protokolle aneinander erforderlich, was üblicherweise durch sogenannte Gateways erfolgt. Um einen möglichst unbehinderten Datenaustausch zwischen modernen Kommunikationssystemen zu ermöglichen, die einen hohen Grad an Komplexität und eine Vielzahl von Funktionen aufweisen, werden die verschiedenen Funktionen schematisch Schichten zugeteilt und für die verschiedenen Schichten werden angepaßte Protokolle definiert. Das verbreitetste derartige System ist das von der ISO (International Standard Organization) festgelegte OSI-Referenzmodell (Open Systems Interconnection), ein Siebenschichtenmodell der Kommunikation.

Eine Verknüpfung von Kommunikationssystemen kann prinzipiell auf jeder der Schichten erfolgen. Dabei treten Kommunikationsrechner miteinander in Verbindung, welche die benötigten Protokolle zur Verfügung stellen. Üblicherweise werden letztere mit einem Prozessor realisiert, der daneben noch weitere Funktionen übernimmt, beispielsweise eine gewünschte Anwendung abzuarbeiten. Dies hat jedoch einige entscheidende Nachteile, insbesondere wenn gleichzeitig viele von verschiedenen Schichten herrührende Kommunikationsbeziehungen zu verarbeiten sind. So wird der Rechner durch die Gateway-Funktionen, das heißt die ständig nötigen Protokollumformungen belastet, was zu Lasten der übrigen Rechenanwendungen geht. Die einzelnen Protokolle, obwohl funktionell und vom Ablauf her voneinander unabhängig, sind zeitlich gekoppelt; weiter sind sie einem einheitlichen Betriebssystem unterworfen, obwohl sie unterschiedliche Anforderungen an ein Betriebssystem stellen.

Bei der Datenübertragung über Netze, zu denen die verschiedensten Benutzer Zugang haben, stellt sich immer auch die Frage der Zugangskontrolle bzw. der Datensicherheit. Bisher bekannte Lösungsansätze basieren auf funktionalen Erweiterungen auf einer oder mehreren Protokollschichten oder definieren spezielle Protokoll-Zwischenschichten. Derartigen Maßnahmen haften jedoch einige Nachteile an. Da noch keine endgültigen Normen für die erwähnten Zusätze vorhanden sind, besteht die Gefahr der Inkompatibilität wegen unterschiedlicher Realisierungen. Eine garantierte Sicherheit ist auf dieser Basis nicht zu erreichen. Und nicht zuletzt erhöhen die zusätzlichen Sicherheitsfunktionen die Komplexität der Protokolle und erfordern größere Prozessorleistung.

Es besteht daher die Aufgabe, einen Kommunikationsrechner so zu konzipieren, daß er durch die Bearbeitung der Protokolle nicht über Gebühr belastet wird und überdies höchstmögliche Datensicherheit bietet.

Die Aufgabe wird grundsätzlich durch die kennzeichnenden Merkmale gemäß Patentanspruch 1 gelöst. Die gewünschte Datensicherheit wird durch die Ausgestaltung gemäß Anspruch 3 erreicht.

Der vorgeschlagene Kommunikationsrechner zeichnet sich durch eine Mehrzahl von Prozessoren aus, die je für die Verarbeitung der Daten auf zugeordneten Protokollschichten zuständig sind. Eine bevorzugte Ausführungsform sieht für jede Protokollschicht einen eigenen Prozessor vor. Diese Anordnung ermöglicht zeitlich voneinander unabhängige Bearbeitungen, basierend auf angepaßten Betriebssystemen für jeden Prozessor. Die gegenseitige Beeinflussung der Protokolle entfällt, die Verzögerungen bleiben gering, was einen hohen Datendurchsatz ergibt.

Die DE-A-41 20 398 beschreibt eine Datenverarbeitungsanlage, bei der zwischen der zentralen Verarbeitungseinheit (CPU), also dem Prozessor, und dem Datenbus eine Ent-/Verschlüsselungseinrichtung geschaltet wird. Auf diese Weise wird ein unautorisierter Zugriff auf den Prozessor abgewehrt. Dieses Prinzip läßt sich auf einen oder mehrere Prozessoren des erfindungsgemäßen Kommunikationsrechners anwenden, wodurch sich die angestrebte Datensicherheit erreichen läßt.

Die Erfindung wird am Beispiel des eingangs erwähnten OSI-Referenzmodells anhand der nachstehenden Figuren näher erläutert. Dabei zeigen:

Fig. 1 einen schematischen Ausschnitt aus dem erfindungsgemäßen Kommunikationsrechner, und

Fig. 2 den Aufbau der Telegramme über die 7 OSI-Schichten mit Verschlüsselung auf zwei Ebenen.

Die Fig. 1 zeigt den erfindungswesentlichen Teil einer als Kommunikationsrechner dienenden Datenverarbeitungsanlage. An einen Bus 8 sind nebst anderen, nicht gezeichneten Schaltungen wie Arbeitsspeicher und Peripheriesteuerungen insgesamt acht Prozessoren angeschlossen. Jeder der acht Prozessoren ist zuständig für die Bearbeitung der Telegramme der entsprechenden Schicht des OSI-Referenzmodells, nämlich der Anwendungsprozessor 7 für die Schicht 7, den "Application Layer", der Darstellungsprozessor 6 für die Schicht 6, den "Presentation Layer", der Sitzungsprozessor 5 für die Schicht 5, den "Session Layer", der Transportprozessor 4 für die Schicht 4, den "Transport Layer", der Internetzwerkprozessor 3c und der Netzwerkprozessor 3a für die Schicht 3, den "Network Layer", der Datensicherungsprozessor 2 für die Schicht 2, den "Datalink Layer" und der Bitübertragungsprozessor 1 für die Schicht 1, den "Physical Layer". Der Gebrauch von zwei Prozessoren auf der Netzwerkebene entspricht der Unterteilung dieser Schicht in die Unterschichten 3a, b für die Intranetzwerkkommunikation bzw. 3c für die Internetzwerkkommunikation, welche bevorzugt für die Netzverknüpfungen über Gateways benutzt wird.

Es sei an dieser Stelle festgehalten, daß die gezeigte Aufteilung zwar bevorzugt aber nicht zwingend ist. Im Sinne der Erfindung ist auch das Zusammenlegen von Prozessoren möglich, namentlich solcher für Protokolle, die ähnliche Anforderungen an die Arbeitsweise des Prozessors stellen, wie z. B. der Darstellungsprozessor 6 und der Sitzungsprozessor 5. Die voneinander unabhängige Bearbeitung ist damit zwar nicht mehr in vollem Maß gegeben, doch kann unter Umständen eine Überkapazität von Prozessorleistung vermieden werden.

Eine Besonderheit im Dienste der Datensicherung stellt die Kryptierung auf einzelnen Schichten dar, was beispielsweise durch eine Ent- und Verschlüsselungseinrichtung 9 bzw. 9' bewerkstelligt wird, die zwischen den Transportprozessor 4 und den Bus 8 bzw. den Datensicherungsprozessor 2 und den Bus 8 geschaltet ist. Die zwischen dem Prozessor 4 und der Ent-/Verschlüssel-

ungseinrichtung 9 verkehrenden Daten und Befehle 10 sind unverschlüsselt. Die Daten und Befehle 11, die von der Ent-/Verschlüsselungseinrichtung 9 an den Bus 8 gelangen, können je nach Bedarf verschlüsselt sein oder nicht. Die Wirkungsweise der Verschlüsselung wird anhand der Erläuterung zur Fig. 2 näher ausgeführt. Auch hier sei darauf hingewiesen, daß die gezeichnete Anordnung Beispielcharakter hat. Das Kryptieren kann auch auf andere Weise bewerkstelligt werden. Ent-/Verschlüsselungseinrichtungen 9 können auch anderen Prozessoren und in insgesamt anderer Anzahl zwischengeschaltet werden. Bevorzugt ist dabei insbesondere der Internetzwerkprozessor 3c, weil dieser die Gateways zu fremden Netzwerken bearbeitet. Die Ent-/Verschlüsselungseinrichtung 9 ist auch in der Lage, die Daten ohne Beeinflussung direkt weiterzugeben.

Der physikalische Aufbau des Mehrprozessor-Rechners kann auf vielfältige Weise erfolgen. Dies reicht von Baugruppen in eigenständigen, voneinander getrennten Geräten über rechnerbusverknüpfte Prozessoren in einem Gerät bis zu Prozessoren auf einer gemeinsamen Leiterplatte, wobei Mischformen denkbar sind.

Die Fig. 2 zeigt schematisch den Aufbau der Telegramme, wie sie gemäß den Vorgaben des OSI-Referenzmodells auf den einzelnen Ebenen strukturiert und ausgewertet werden. Auf der rechten Seite sind wiederum die acht Prozessoren gezeichnet, wie sie im Zusammenhang mit Fig. 1 beschrieben wurden, diesmal sinnfälliger auf verschiedenen Ebenen übereinander angeordnet. Die anfallenden Daten einer Anwendung werden vom Anwendungsprozessor 7 in ein protokollgerechtes, genormtes Anwendungstelegramm 17 gepackt, das zwei Teile einschließt, die Anwendungs-Nutzdaten, kurz 7-Daten 27 genannt, und deren sogenannter Header, die Anwendungs-Kopfdaten, hier kurz 7-Kopf 37 genannt. Auf der darunterliegenden Schicht 6 wird dieses Telegramm als Ganzes übernommen. Der Darstellungsprozessor 6 packt die auf dieser Ebene anfallenden Daten in ein protokollgerechtes, genormtes Darstellungs-Telegramm 16, in dessen Darstellungs-Nutzdaten, kurz 6-Daten 26, das ganze Anwendungs-Telegramm 17 der überlagerten Schicht 7 enthalten ist, und das mit den Darstellungs-Kopfdaten, kurz 6-Kopf 36, versehen ist. Dieses Verfahren setzt sich über die fünfte Stufe, die Sitzungs-Schicht mit dem Sitzungs-Telegramm 15 bestehend aus den 5-Daten 25 und dem 5-Kopf 35, zur vierten Stufe, der Transport-Schicht fort.

Hier nun, in Übereinstimmung mit der für die Fig. 1 getroffenen Annahme, ist durch die erste Schraffur das Kryptieren angedeutet, das Verschlüsseln der Daten bzw. deren Entschlüsseln, wenn der Vorgang in umgekehrter Richtung betrachtet wird. Der Transportprozessor 4 ist ein Kryptoprozessor, wie er beispielsweise durch eine Anordnung gemäß Fig. 1 realisiert wird. Seine Ausgangsdaten, das Transport-Telegramm 14, liegen verschlüsselt vor. Die verwendeten Protokolle und deren Funktionen werden dadurch nicht beeinflusst. Die Daten, die an die darunterliegenden Schichten zur weiteren Bearbeitung übergeben werden, sind jetzt jedoch verschlüsselt und nur vom Empfängerprozessor der entsprechenden Schicht wieder zu entschlüsseln. Ein berechtigter Teilnehmer im Kommunikationssystem muß also ein Kommunikationsrechner sein, der über einen Kryptoprozessor auf derselben Ebene und den entsprechenden Schlüssel verfügt. Gemäß der dem Schichtenmodell zu Grunde liegenden Vereinbarung, werden Kopf und Daten, also das ganze Telegramm einer Schicht von der darunterliegenden Schicht immer als

Daten betrachtet. Die im Beispiel auf der Transportebene vorgenommene Kryptierung ist auf der darunterliegenden Netzwerkebene nicht erkennbar und ebenso wenig auf den noch weiter unten liegenden Ebenen. An die darüberliegende Sitzungsebene hingegen werden nur entschlüsselte Daten weitergegeben.

In Fortsetzung des beschriebenen Verfahrens wird ein bereits teilweise verschlüsseltes Intranetzwerktelegramm 13a auf der Datensicherungsebene, auf der gemäß Annahme wiederum ein Kryptoprozessor wirkt, Teil des Datensicherungs-Telegramms 12, das als Ganzes verschlüsselt ist. Ein Teil der 2-Daten 22 ist nun doppelt verschlüsselt, während der 2-Kopf 32 und der restliche Teil der 2-Daten 22 einfach verschlüsselt sind. Der Bitübertragungsprozessor 1 bereitet diese Daten dessen ungeachtet zum Bitübertragungstelegramm 11, bestehend aus dem 1-Kopf 31 und den 1-Daten 21 auf. Fehlt bei einem Teilnehmer am Kommunikationssystem der Kryptoprozessor auf der Datensicherungsebene oder dessen Schlüssel, kann er gar nicht kommunizieren. Fehlt der Kryptoprozessor auf der Transportebene, hält zwar die Verbindung, die übertragene Information ist aber für ihn nicht zugänglich.

Selbstverständlich ist die Kryptierung auf mehreren oder sogar allen Schichten möglich. Von besonderer Bedeutung ist die Internetzwerkschicht 3c, die für die Kopplung unterschiedlicher Netze in einem Netzwerkverbund vorgesehen ist. Über entsprechenden Gateways sind derart Übergänge zwischen öffentlichen, privaten und militärischen Netzen möglich, was eine zuverlässige Kontrolle über die Zugangsberechtigung bedingt.

Gateways sind gemäß dem OSI-Referenzmodell prinzipiell auf allen Schichten möglich. Die Verwendung spezifischer Prozessoren für eine bestimmte Schicht ermöglicht es, die Telegramme dieser Schicht direkt zu verarbeiten und so Protokollumwandlungen zu umgehen. In einem Verbund von Kommunikationsrechnern mit Prozessoren für fest zugeordnete Protokollschichten können die Rechner über Gateways auf beliebigen Protokollschichten miteinander in Verbindung treten, ohne rechnerinterne Protokollanpassungen je nach Schicht vornehmen zu müssen. Dabei läßt sich in Verbindung mit der Kryptierung auch dem Aspekt der Datensicherheit Rechnung tragen.

#### Patentansprüche

1. Kommunikationsrechner für den Betrieb in einem Rechnerverbund mit einem Datenaustausch auf mehreren Schichten anhand definierter Protokolle, mit einem Adreßbus und einem Datenbus (8), an die mindestens ein Prozessor, Arbeitsspeicher und Steuerschaltungen für Peripheriegeräte angeschlossen sind, dadurch gekennzeichnet, daß im Kommunikationsrechner je ein Prozessor (1, 2, ..., 7) für die Datenverarbeitung auf einer oder einer fest zugeordneten Gruppe von Protokollschichten vorhanden sind.
2. Kommunikationsrechner nach Anspruch 1, dadurch gekennzeichnet, daß im Kommunikationsrechner je ein Prozessor (1, 2, ..., 7) für die Datenverarbeitung auf genau einer fest zugeordneten Protokollschicht vorhanden ist.
3. Kommunikationsrechner nach Anspruch 1 oder 2, dadurch gekennzeichnet, daß die zwischen einem bis allen ausgewählten Prozessoren (2, 4) und dem Datenbus (8) übertragenen Informationen (11) verschlüsselt sind.

4. Kommunikationsrechner nach Anspruch 3, dadurch gekennzeichnet, daß die zwischen dem für die Protokollschicht (3)c nach dem ISO/OSI-7-Schichtmodell zuständigen Prozessor (3c) und dem Datenbus (8) übertragenen Informationen (11) 5 verschlüsselt sind.

5. Kommunikationsrechner nach einem der vorstehenden Ansprüche, dadurch gekennzeichnet, daß er über ein Gateway auf einer beliebig wählbaren Schicht, der ein eigener Prozessor zugeordnet ist, 10 kommuniziert, wobei die Telegramme (11, 12, ..., 17) einer Protokollschicht direkt vom zuständigen Prozessor (1, 2, ..., 7) verarbeitet werden, wodurch Protokollumwandlungen entfallen.

---

Hierzu 2 Seite(n) Zeichnungen

---

15

20

25

30

35

40

45

50

55

60

65

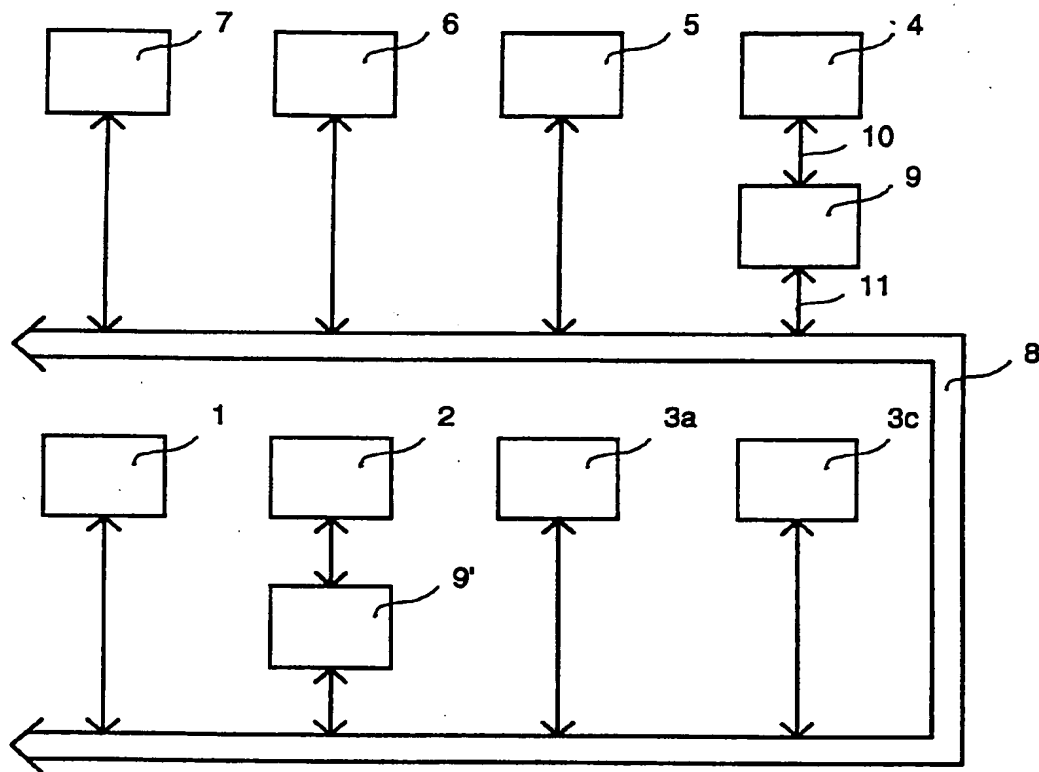


Fig. 1 ✕

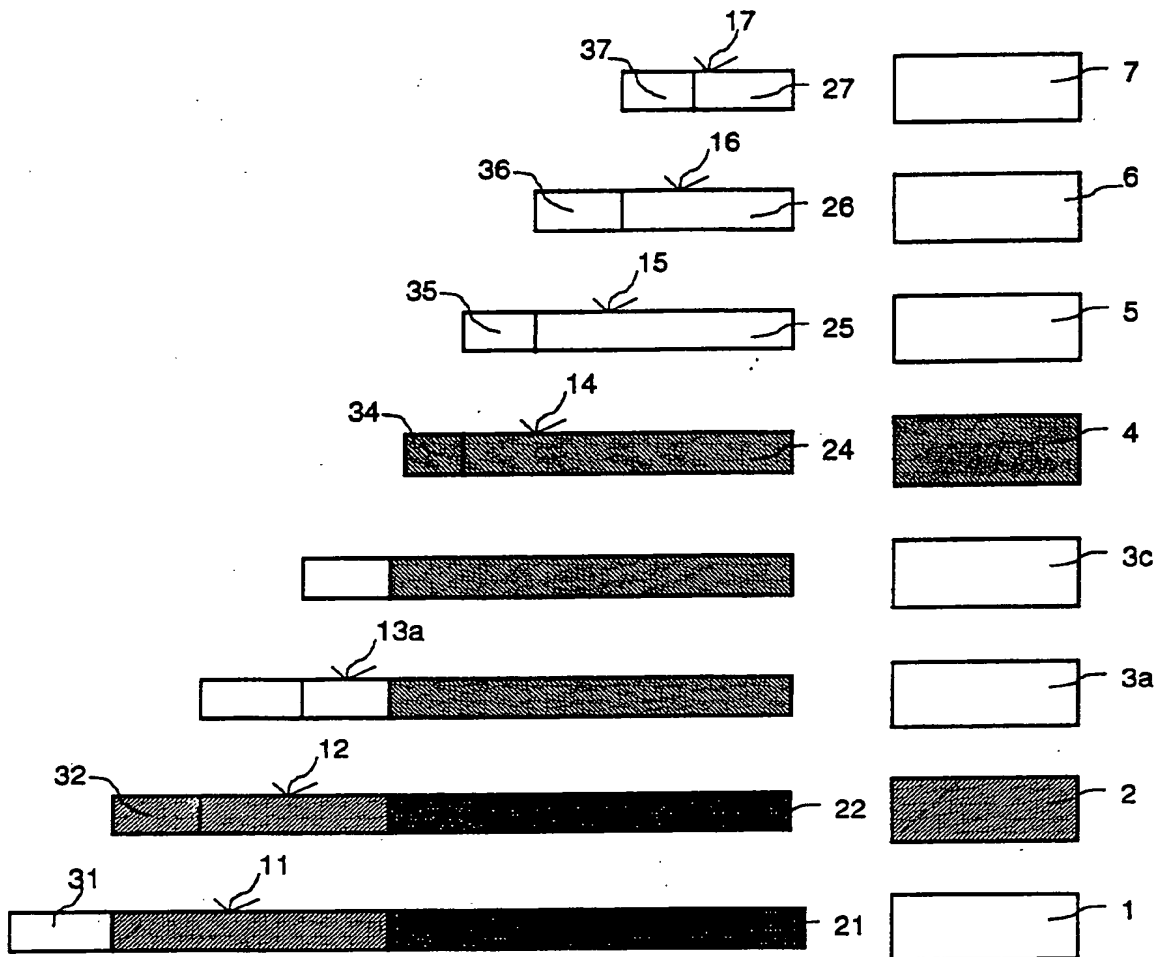


Fig. 2